2005-09

How can we improve information sharing among local law enforcement agencies?

Miller, Patrick E.

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HOW CAN WE IMPROVE INFORMATION SHARING AMONG LOCAL LAW ENFORCEMENT AGENCIES?

by

Patrick Miller

September 2005

Thesis Advisor:	Chris Bellavita
Second Reader:	Dave Brannan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: How Can We Improve Information Sharing Among Local Law Enforcement Agencies?			**5. FUNDING NUMBERS**
6. AUTHOR(S) Patrick Miller			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Ventura Police Department 1425 Dowell Dr, Ventura, Ca 93003			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The events of 9/11 and subsequent examination of the intelligence community in the United States have clearly identified several areas that require immediate repair. While we have, on the federal, state and local levels, a complex system of collecting, developing, and analyzing intelligence that can be used to prevent terrorist attacks, we do not have an accompanying system that shares intelligence information throughout the law enforcement community.

The purpose of this thesis is to review information sharing between federal, state and local law enforcement agencies and to suggest methods to improve that capability.

In the aftermath of the September 11th attacks, authorities uncovered patterns of suspicious activity occurring in places such as Maryland, Florida, and New Jersey. These activities included individuals paying cash for plane tickets, taking flight lessons, inquiring about crop duster planes, and frequenting drug stores.

Taken individually, these incidents were not overly suspicious; nor were they seen as serious when reported to authorities. Yet, all together they illustrate at best highly suspicious behavior, and at worst a picture of a master plan of prospective criminal activity. When collecting data on terrorist potential, one isolated incident in a local jurisdiction may not have obvious significance, but the ability to view all incidents together across cities or states might paint a more complete picture. Agencies are now recognizing the benefits of data sharing across institutions and jurisdictions.

14. SUBJECT TERMS Information Sharing – Intelligence Sharing- Local Law Enforcement – Terrorism Working Group – Fusion Center -			**15. NUMBER OF PAGES** 85
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HOW CAN WE IMPROVE INFORMATION SHARING AMONG LOCAL LAW ENFORCEMENT AGENCIES?

Patrick E. Miller
Chief of Police, Ventura Police Department
B.S., California Lutheran University, 1975
MPA, Pepperdine University, 1981

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN NATIONAL SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2005**

Author: Patrick Miller

Approved by: Dr. Chris Bellavita
Thesis Advisor

Dr. David Brannan
Second Reader

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The events of 9/11 and subsequent examination of the intelligence community in the United States have clearly identified several areas that require immediate repair. While we have, on the federal, state and local levels, a complex system of collecting, developing, and analyzing intelligence that can be used to prevent terrorist attacks, we do not have an accompanying system that shares intelligence information throughout the law enforcement community.

The purpose of this thesis is to review information sharing between federal, state and local law enforcement agencies and to suggest methods to improve that capability.

In the aftermath of the September 11th attacks, authorities uncovered patterns of suspicious activity occurring in places such as Maryland, Florida, and New Jersey. These activities included individuals paying cash for plane tickets, taking flight lessons, inquiring about crop duster planes, and frequenting drug stores.

Taken individually, these incidents were not overly suspicious nor were they seen as serious when reported to authorities. Yet, all together they illustrate, at best, highly suspicious behavior and, at worst, a picture of a master plan of prospective criminal activity. When collecting data on terrorist potential, one isolated incident in a local jurisdiction may not have obvious significance, but the ability to view all incidents together across cities or states might paint a more complete picture. Agencies are now recognizing the benefits of data sharing across institutions and jurisdictions.

The success of the fusion center concept rests in the ability of the Office of the Director of National Intelligence, the Department of Homeland Security and the FBI to make a collaborative decision on what system(s) would best meet these requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis represents the culmination of quite a journey. It has certainly been an honor to participate in this exemplary effort to educate professionals from all disciplines and walks of life. There are many to whom I owe my thanks and gratitude.

My thanks to all of those at the Naval Postgraduate School and the Office for Domestic Preparedness (ODP) at the Department of Homeland Security. A Special appreciation to Dr. Paul Stockton for his vision and tenacity in developing this program at NPS and his thoughtful insight into the intelligence and information sharing business.

To Dr. Chris Bellavita for his patience, understanding and valuable input throughout the 18 months.

To all of my classmates in 0401 and 0402 for your genuine contribution to the security of this country and your 100% effort, it was amazing at times.

I cannot miss this unique opportunity to mention three very special people that I have had the honor of meeting during the last year and one half. They bring all that is good about public safety and they are shining examples of what it means to give your all for country, profession and partner. Deputy Assistant Chief Joe Pfeifer, Commander Cathy Lanier and Special Agent in Charge Greg Jones…my thanks and my admiration.

To the City of Ventura….retired Chief Mike Tracy for his relentless pursuit of excellence and his encouragement to give this a try and to City Manager Rick Cole for his vision and realization that it is a big world out there.

To Mike Nocita – for the editorial assistance.

To Dr. Dave Brannan – Old friends are the best ones. Thanks partner.

To my family. Once again they have endured and persevered. Thank you very much.

Finally, my Little Buddy. We're doing this for you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Effective terrorism-related prevention, protection, preparedness, response, and recovery efforts depend on timely, accurate, and actionable information about who the enemies are, where and how they operate, how they are supported, the targets the enemies intend to attack, and the method of attack they intend to use. This information should serve as a guide for efforts to:

- Rapidly identify immediate and long-term threats
- Identify persons involved in terrorism-related activities
- Guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

Terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism–related information. It can come through the efforts of the intelligence community; Federal, State, tribal, and local law enforcement authorities; other government agencies (e.g., transportation, healthcare, general government), and the private sector (e.g., transportation, healthcare, financial, Internet/information technology).

For the most part, terrorism-related information has traditionally been collected outside of the United States. Typically, the collection of this type of information was viewed as the responsibility of the intelligence community and, therefore, there was little to no involvement by most State and local law enforcement entities. The attacks of September 11, 2001, however, taught us that those wanting to commit acts of terrorism may live in our local communities and be engaged in criminal and/or other suspicious activity as they plan attacks on targets within the United States and its territories.

As a pointed reminder and using Europe as an example, the following is an excerpt from Der Speigel, July 12, 2005:

> The scenario on Al-Hindi's hard drive is reminiscent of the July 7 bomb attacks on the London Tube and a double-decker bus. By last Sunday, it was still unclear who had detonated the bombs but the attacks, say British security experts, bear the handwriting of Islamic terrorists. Perhaps as

> frightening as the bombs themselves is the fact that intelligence agents and investigators in Great Britain and throughout Europe had no idea an attack was imminent -- and this despite the fact that they have spent years trying to infiltrate the Islamic extremist network in Europe. Indeed, one month before the attacks, Scotland Yard lowered its terrorism alert level for the British capital by a notch.
>
> But al-Qaida in Europe is not an organization that readily lends itself to infiltration or wire-tapping. That's because al-Qaida is not a fixed structure, but rather an ideology that has managed to fascinate young Islamists from Gibraltar to Scandinavia. These young terrorists may know each other and even cooperate when it comes to logistics, but they operate in small, flexible independent groups, making them almost impossible to catch.
>
> It has long been clear that Europeans, especially Britons, could be attacked at any time. The attacks in Istanbul in November 2003 (57 dead) and the train bombings in the Madrid suburbs on March 11, 2004 (191 dead) were only the beginning. "No country," says EU counterterrorism coordinator Gijs de Vries, "can nurture false hopes of being safe." German Interior Minister Otto Schily, who flew to London on Friday to meet with his British counterpart, warns that "radical Islamists have also explicitly named Germany as an enemy.
>
> The Old Continent, once a place for Muslim extremists to withdraw and recuperate, has turned into a battlefield. Gilles Kepel, a French expert on Islam, is already referring to the current situation as a "fight for Europe."[1]

Important intelligence that may forewarn of a future attack may be derived from information collected by State, tribal, and local government personnel through crime control and other routine activities and/or by people living and working in our local communities. Successful counterterrorism efforts require that Federal, State, tribal, local, and private-sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences in support of prevention, response, and consequence management efforts.

[1] Andreas Ulrich, "Radical Islam's Rising War on Europe," *Der Speigel*, July 12, 2005, http://www.salon.com/news/feature/2005/07/12/terrorism_eu/print.html, accessed July 12, 2005.

A. PURPOSE

The purpose of this project was to identify methods of improving information sharing at the federal, state and local level. What I offer are a set of guidelines that can lead to that improvement and facilitate a more rapid, accurate means of sharing data and intelligence.

In preparation for this project, I spoke with or received information from 243 local Police Chiefs and Sheriffs throughout California.

While the original purpose of this thesis was to review the local law enforcement approaches to homeland security and to examine a leadership model that may offer the best method of promoting the requisite coordination and collaboration, I found that more basic concerns dominated the local perspective.

While the leadership discussion was certainly intriguing and worthy of study, I found that the essential local concerns dealt with information and intelligence sharing in its simplest form. There was a profound belief amongst law enforcement leaders in California that the essential mechanisms for information sharing are poor at best and arriving at some consensus on how to fix that problem was far more important that examining leadership models and future impacts.

As I discuss later in this project, there was a gradual refinement of the scope of the research from an overall perspective of three over-arching models – Super-Agency, Legal and Database approach – to a more realistic, simplified version of a fusion center concept.

I would be remiss, however, if I did not include a small portion of the leadership discussion, as I firmly believe that without dynamic law enforcement leadership, we will replicate the past mistakes.

I asked each Chief/Sheriff to respond to the question…What leadership model should law enforcement adopt to meet the challenges of homeland security? They were very consistent in their response that transformational leadership would be required. (Approximately 94% responded affirmatively). While I discuss the transactional-Transformational leadership models later in this thesis, it is also interesting to note that

these law enforcement leaders were nearly unanimous in their belief that even though transformational leadership is required, very few practiced it.

1. A Promising Approach

It is generally accepted that information sharing at the federal, state and local level has been deficient. The myriad of federal investigations has clearly defined the scope of that problem.

A more promising approach to information sharing would build upon what few successes law enforcement has had with "vertical" integration - crossing federal, state, and local levels of government. Bodrero[2] as well as White[3] recommend using the six-region information network known as RISS (Regional Information Sharing Systems). The RISS Network was designed for sharing criminal intelligence, primarily about gang crime, hate crime, and cyber-crime, and would provide a model that works and makes effective use of existing intelligence analysts who work for police departments. RISS is the closest thing to a nationwide criminal investigation network.

Another approach is to build on the War on Drugs as an intelligence model, and NDIC (National Drug Intelligence Center) holds some promise for development because it has always involved excellent cooperation between levels of government. In addition, DEA has identified several High Intensity Drug Trafficking Areas (HIDTAs), the El Paso Intelligence Center (EPIC) being most notable, which represent excellent working models of how intelligence analysts, from both law enforcement and the military, can come together to work on a common problem.

In addition, there are numerous states with highly developed criminal intelligence units, such as the New Jersey State Intelligence Unit, which has long had an effective intelligence gathering and analysis capability. Most state police intelligence units maintain liaisons with INTERPOL (International Criminal Police Organization), EUROPOL, FINCEN (Financial Crime Enforcement Network), IALEIA (International Association of Law Enforcement Analysts), and LEIU (Law Enforcement Intelligence Unit). It makes little sense for the federal government to ignore these resources as they represent the "best and brightest" that local law enforcement has to offer.

---

[2] Douglas Bodrero, "Law Enforcement's New Challenge to Investigate, Interdict, and Prevent Terrorism." *The Police Chief* (February, 2002): 41-48.

[3] Jonathan White, *Defending the Homeland* (Belmont, CA: Wadsworth, 2004), 27.

B. CHAPTER BY CHAPTER SUMMARY

Chapter II begins with a perspective not mentioned very often in law enforcement circles, yet was a clear bias of law enforcement leaders with whom I spoke. Terrorism, organized crime, drug trafficking, and arms smuggling are serious challenges confronting American policymakers, and law enforcement has an important--sometimes-central--role in combating each of these threats. That being said, there are two fundamental flaws in that viewpoint, which leads to a discussion of three basic approaches to the law enforcement role…the Super-Agency approach, the legal approach and the database approach. While each has its merit, the database approach tends to support the ultimate conclusion of this thesis – a fusion center or some version of that concept.

Chapter II concludes with a brief review of existing thought regarding the role of leadership in the homeland security/law enforcement arena. While this is certainly an area deserving of further explanation, I do not believe that success is attainable absent the adoption of a fundamental shift in the leadership paradigm. The transformational leader is the new model required to accomplish the fundamental aspects of information and intelligence sharing.

Chapter III examines several existing arrangements that have offered glimmers of hope. There are currently several database approaches that offer promise, yet they remain under-utilized and disconnected. One, the MATRIX system, entered with fanfare and exited in ignominy.

Chapter IV examines the Los Angeles Terrorism Early Warning Group, likely the most successful fusion attempt to date. Driven by the initiative of Lt. John Sullivan, it enhances the intelligence and information sharing capabilities of a large, metropolitan area and is suited toward the resource driven environment that it demands. The LA TEW again offers a glimmer of hope and provides several areas adaptable to the more diverse, smaller agencies that constitute the breadth and depth of the American landscape.

Chapter V is a brief recap of the interviews of California Law Enforcement Leadership that I conducted. While somewhat bleak in its prognosis, it does offer hope in that most of the leadership in California supports some type of unified approach in conjunction with an information sharing mechanism.

Chapter VI offers a compilation of the recommendations proffered by the case studies and leadership input garnered from the interviews conducted over the course of several months. My participation in a Homeland Security Advisory Committee was extremely helpful in distilling the listed bullets. It is meant as a guidepost, not a mandatory step by step process. While some areas may be possible for all jurisdictions, most must be adapted to individual needs and focus areas.

Finally, Chapter VII summarizes the main conclusion of this attempt at consensus. There are other requirements beyond the need to develop a system that is able to capture, analyze and pass along the information from the hundreds of thousands of local law enforcement and government officials working in communities every day. It is also important to have a local mechanism to disseminate the strategic intelligence information that is typically developed by the federal government.

Further, local entities need to be able to collect and disseminate information at the tactical intelligence level. If the collection and analysis system is working properly states can provide valuable pieces of information to the federal government who is in the position to "connect the dots" from a regional or national perspective. Depending on the type of information, regions or counties often can take action independently when an impending attack is discovered or if plans are discovered that do not have national implications.

While the term "fusion" center is congruent with the mission of intelligence and information sharing, the concept is the vital factor, not the name or location.

II. BACKGROUND

A. IMPORTANCE OF LAW ENFORCEMENT AND FOREIGN POLICY

Law enforcement leaders are nearly unanimous in their belief that few tools of U.S. foreign policy are as vitally important and as consistently overlooked as law enforcement on both the federal and local level. Terrorism, organized crime, drug trafficking, and arms smuggling are serious challenges confronting American policymakers, and law enforcement has an important--sometimes-central--role in combating each of these threats. I believe that role suffers, however, from two serious flaws.

First, differences in bureaucratic culture and viewpoints between the law enforcement and national security communities make coordination difficult. Law enforcement agencies generally do not see themselves as components of U.S. foreign policy. Nor does the traditional foreign policy establishment adequately appreciate the distinct culture, capabilities and constraints that characterize U.S. law enforcement agencies. Albeit, the New York Police Department has stepped outside the boundaries of traditional law enforcement and is forging a new role for a municipal police agency. "The NYPD is really cutting edge," Brian Jenkins, a senior advisor of the RAND corporation stated, "They're developing best practices here that should be embraced across the country. The Feds could learn from them."[4]

Second, there are structural impediments to effective coordination between the various law enforcement agencies and the traditional national security apparatus. While many federal law enforcement agencies are beset by turf battles, lack proper civilian oversight and are organizationally ill-suited for integration into the wider foreign policy community, local law enforcement agencies have not adapted the leadership models necessary for success nor properly identified their role in the homeland security system.

Local Law enforcement has also always been a decentralized phenomenon in American society and without a new leadership model and a clearly defined role, it may

4 Brian Jenkins (RAND Corporation), Interview with the National Tactical Officers Association, February 2005.

not be up to the task of collecting, sharing, coordinating, and analyzing the intelligence necessary to successfully assess and respond to modern-day threats.

For most of American history, there has been a bright line between national security threats on the one hand and criminal threats on the other. The former were international, the latter domestic. The international side was the purview of the military and intelligence agencies; the domestic side that of the law enforcement agencies. This separation was primarily intended to prevent military encroachments on civilian authorities and civil liberties. The fear of militarism in American civil society remains deeply embedded in the national consciousness and has long been incorporated into American governance. U.S. government actions are still defined by the Posse Comitatus Act, passed in 1878 to prohibit the military from performing certain domestic police functions.

In recent decades, this bright line has blurred. Traditional crimes in the United States have increasingly been found to have links to criminal networks overseas. Narcotics trafficking, most obviously, cannot possibly be combated by domestic law enforcement operations alone. A bipartisan consensus also has emerged that the threat from foreign narcotics trafficking is not just a law enforcement concern but a matter of national security as well. Thus in 1987, President Reagan overruled his Secretary of Defense and instructed the military to go abroad to help fight the war on drugs.

As technology advanced and borders became increasingly porous after the Cold War, it became increasingly evident that international crime in all of its various forms threatened U.S. national security interests. Sometimes the threats were direct. Terrorists groups like Al Qaeda, no longer as dependent on state sponsorship, began targeting Americans at home and abroad. They also engaged in a host of criminal activities apart from terrorism, from arms trafficking to people smuggling to securities fraud. Vast networks of criminals based in Russia, Nigeria, Latin America, East Asia and elsewhere went global, infiltrating the United States as one of the world's most lucrative targets. Hackers halfway around the world broke into U.S. computer systems, including sensitive systems belonging to the military and intelligence agencies.[5]

[5] David W. Brannan, *Beyond International Terrorism: Thinking About the 'Domestic' vs. 'International' Divide* (Oklahoma City: MIPT, 2003), 3-21.

In the year 2005, with the international threat demanding collaboration and coordination, it is vital that local law enforcement clearly defines its role in the homeland security system. While there may be several different approaches that might be successful, the following three have potential.

B. SUPER-AGENCY APPROACH

While the definition of super-agency is open to considerable and varied discussion, the basic concept of data sharing and intelligence dissemination is not uncommon throughout the world.[6] The idea of some sort of super-agency that tracks the ideological thoughts of its citizens has been considered in the United States for some time. It is implicit in most proposals to federalize, centralize, or consolidate police forces. It is explicit in most proposals to reorganize the intelligence community, such as the 1970 Huston Plan (named after White House staffer Tom Charles Huston) which advocated combining the CIA, FBI, NSA, and DIA or the 1996 Webster report that concluded the current organization of Federal law enforcement needed to be changed.

While far from creating a domestic intelligence super-agency (like MI5 in Britain), the actual creation of the Department of Homeland Security (DHS) was a significant transformation of the government approach. The new department's first priority became protection of the nation against further terrorist attacks, followed by additional duties for intelligence and threat analysis, guardianship of borders and airports, protection of critical infrastructure, and emergency response coordination. Along with the Coast Guard and Secret Service, twenty-two (22) separate agencies were consolidated into the DHS, and housed in one of four major directorates: Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Analysis and Infrastructure Protection.

That is not to say success has followed nor did the consideration clearly define the current or future role of local law enforcement in the homeland security apparatus. One of the most frequent criticisms of DHS is not that it's too big (America has had similar super-agencies such as LEAA, the Law Enforcement Assistance Administration,

[6] The English, French and German intelligence are but a few examples of countries that employ this concept.

established under the 1968 Crime Control and Safe Streets Act and dismantled in 1980 with NCJRS remaining as a remnant), but that it is too small, and does not include two agencies, CIA and FBI, which seem like logical choices for inclusion in DHS due to their poor record of information sharing and collaboration.[7]

The CIA and FBI are already overwhelmed by a sea of information, and DHS was designed to use new and different intelligence to uncover threats. As the National Strategy for Homeland Security makes clear, existing agencies like the CIA and FBI were to enhance their analytic capabilities and new agencies, like the DHS, were to build new ones.

DHS was formed without benefit of a strategy to guide its structure and activities. Functions were merged for which a clear strategic case had not been made. DHS contains many activities that detract from homeland security, including many that have little day-to-day connection with one another. For example, DHS includes maritime safety and drug interdiction, child pornography integration, and research and non-native plant and pest eradication efforts, just to name a few. Other functions, such as chemical and biological research, environmental measurement, and law enforcement training may be linked to homeland security, but just because a variety of functions contribute to homeland security does not mean that they necessarily need to be under common organizational control.

DHS does not have viable mechanisms to coordinate with those federal agencies not under its jurisdiction. Nor can it rely on other Executive Branch offices that might serve that function. Realigning and combining similar agencies in DHS may improve some operations after the dust of bureaucratic disruption finally settles, but it will not solve the problem of coordination with the other federal agencies, state and local governments, and other entities responsible for key homeland security activities. (Such as the 28 disparate agencies listed by Dr. Pelfrey described below). While units from eight departments merged into DHS, most of the U.S. government capacity key to the homeland security problem is left out. As noted, the FBI and CIA will remain external to the department. Counter-terrorism law enforcement is under Justice. Many bioterrorism

[7] *The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission Report),* (Fifth Annual Report, RAND Corporation, December 15 13, 2003), http://www.rand.org/nsrd/terrpanel/.

functions remain at HHS. Defense has major homeland security functions. By the Administration's own count, more than three-quarters of the agencies involved in homeland security remain outside the department. It was just this dispersal of homeland security-related functions that was the reason for centralizing the coordinating functions in the White House under the initial Office of Homeland Security.

Perhaps, the most important function of DHS was domestic counterterrorism, an idea that encompasses the notion of an informed and proactive citizenry (informed via new Alertness and Awareness systems) who see something unusual and report it to the appropriate authorities. This is very similar to the voluntary cooperation that police need from citizens for crime reporting, or for the success of any community policing effort. It generates the question of how far law enforcement ought to go with investigating suspicious, non-criminal activity.[8]

Clearly, the purpose of these non-criminal investigations is to identify, halt, and where appropriate, prosecute terrorists as well as those who provide them logistic support. It primarily involves a tracking mission for local law enforcement, and only secondarily a prosecutorial mission, or bringing terrorists to justice. It is, in short, what Jonathan White calls the "Eyes and Ears" approach to the role of police in intelligence gathering.[9] It is a system of detecting hostile intent. It is interesting to note that a number of initiatives have been designed to promote individual citizen involvement, such as the following:

- Citizen Corps - volunteers who participate in community-level homeland security efforts
- Volunteers in Police Service (VIP)- civilian police who perform non-sworn functions of policing
- Medical Reserve Corps - retired healthcare providers who augment disaster responses
- Operation TIPS (Terrorist Information and Prevention System) - reporting of suspicious activities

[8] IACP Criminal Intelligence Sharing Report, August 2002.

[9] White, *Defending the Homeland*, 40.

- Community Emergency Response Teams (CERT) - training programs in local communities
- Neighborhood Watch - incorporation of terrorism prevention into its mission via local sheriffs
- Infragard - private sector and academic partnering for cyberspace security

The most frequent criticism of initiatives like the above (especially Operation Tips) is that they smack of police state measures, reminiscent of Nazi Germany, Stalinist Russia, or America's own experience with COINTELPRO ("counterintelligence program") of the 1960s that collected files on some 62,000 suspicious Americans.[10] How to incorporate citizen reporting of suspicious behavior into a system of intelligence and law enforcement remains the central dilemma. Without guidelines, laws, constitutional safeguards, and perhaps training of civilians, the citizen role in domestic counterterrorism may be doomed to defeat on fears that it promotes domestic spying.

C. LEGAL REFORM APPROACH

The idea of establishing new laws and legal guidelines is also not a new concept and has had advocates in the past. In 1967, a Supreme Court decision (the Katz case) condemned warrantless electronic surveillance and the following year, the Omnibus Crime Control and Safe Streets Act established probable cause as the standard for obtaining a wiretap against U.S. citizens. A 1969 case (the Alderman case) ruled that the methods and transcripts of a wiretap should be open in court for public and legal scrutiny. This jeopardized exposure of ongoing intelligence operations, so Attorney General Mitchell established the "Mitchell Doctrine," which insisted that the President, acting through the Attorney General, had the inherent constitutional power to authorize warrantless, secret surveillance in the name of national security or for purposes of pure or preventive intelligence. A number of court cases followed, all along the lines of the judiciary warning the executive branch of government to avoid using foreign intelligence

[10] Church Committee Final Report, "Intelligence Activities and the Rights of Americans." April 23, 1976, http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportfindings.htm.

techniques in domestic cases. In 1972, the Court (in the Keith case) disposed of the Mitchell doctrine, and in the 1973 acquittal of Daniel Ellsberg, the President was determined not to be immune from civil liability for authorizing an illegal wiretap. Watergate, which is actually closely connected to the Ellsberg case, but technically refers to the 1972-1974 period most remembered for a break-in and bugging of Democratic Party headquarters, signaled an end to abuses in the name of national security along with claims of executive immunity.[11]

In 1974, Congress passed the Privacy Act which forbade any federal agency from collecting information about the political and religious beliefs of individuals unless in connection with a bona fide criminal investigation, and in 1975, the Freedom of Information Act, allowed individual access to any personal information which might be secret in the name of national security and applied it to the FBI. The final separation of domestic and foreign intelligence came in 1978 with the Foreign Intelligence Surveillance Act (FISA), which lead to the current amendments in FISA and the Patriot Act of 2001, foundations for modern-day legal approaches to domestic security.

The Patriot Act of 2001 can be seen as another amendment to FISA because under the latter, agencies do not need probable cause to gather intelligence if their targets are operating as agents of foreign powers. It is also true that modern (sub-national) terrorists do not usually work for a foreign power but for some nebulous cause.[12] Specifically, the Patriot Act enhances roving surveillance authority and streamlines wiretap authorizations, sets up anti-terrorism asset forfeiture procedures, approves detention of suspected terrorists, removes obstacles to investigating terrorism, increases the penalties for terrorist crimes, removes any statute of limitations, encourages federal involvement in domestic preparedness exercises, and supports activities by the Department of Homeland Security. More significantly, Title I (Intelligence Gathering) of the Patriot Act permits disclosure of foreign intelligence information to any domestic or law enforcement intelligence operation. It permits foreign intelligence techniques, which are generally more aggressive, to be used for criminal justice purposes and it maintains the secrecy of the intelligence apparatus (compared to the Mitchell Doctrine).

---

[11] Pentagon Papers, New York Times, 1971, http://www.infoplease.com/ce6/history/A0838198.html.

[12] Brannan, op. cit. and Bruce Hoffman, *Combating Terrorism, in Search of a National Strategy*, House Committee on Government Reform, March 2001.

The Patriot Act replaces probable cause with a showing of need for an ongoing terrorism investigation and goes a step further by placing a gag order on the person served with the warrant.[13] That person cannot notify the real target of the investigation, or in any way disclose what information law enforcement was seeking. It amends the Family Educational Rights and Privacy Act, and forces school officials to release information and authorizes law enforcement officials to obtain information on use of library resources, books, and Internet usage. Again, school officials are prohibited from disclosing what was the object of the law enforcement inquiry.[14]

The basic dilemma, as White points out, is a legal one.[15] Law enforcement has for years been accustomed to working within legal constraints, collecting evidence that can be used for prosecution in a criminal court. There is a natural terminus to a criminal investigation. The intelligence community has been accustomed to working with few legal constraints, and there is no natural terminus, or end, to an intelligence investigation. Criminal intelligence is governed by constitutional rules of evidence; national security intelligence is not. Going to trial in a terrorism investigation often means exposing the intelligence sources for the sake of a criminal conviction. This irony, as well as other twists having to do with military tribunals, has produced some rather strange effects in the war on terrorism -- American citizens being detained like prisoners of war and foreigners being treated like citizens in criminal courts. Terrorist groups (according to al Qaeda's training manual)[16] instruct their captured agents to make a mockery of justice systems - to insist they were tortured or mistreated, to learn the names of their captors and lie about them, and to use religion at every turn to their advantage. There are other factors that dampen the prospects for successful use of law enforcement for intelligence purposes, and White indicates the following:

- Police do not have the academic credentials or higher order critical thinking skills to understand the root causes of terrorism, its complexities,

---

[13] USA PATRIOT Act, Section 501(d) states: "No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

[14] For a discussion of the controversial issues covered here, see James D. Torr (ed.), *Homeland Security* (New York: Thompson Gale, 2004).

[15] White, 43.

[16] Al-Qaeda Training Manual, (http://www.usdoj.gov/ag/trainingmanual.htm), March 2005.

or the ability to distinguish between terrorist sympathizers and criminal terrorists

- Police are trained in reasonable suspicion and probable cause to make stops, ask questions, detain, infiltrate, and collect information, but intelligence work requires neither standard in the ongoing collection of vast amounts of non-criminal information
- Police agencies are fiercely autonomous, competitive, turf-conscious, mistrustful, and attuned to local politics with little or no interest in thinking outside their jurisdiction and/or partnering with non-police agencies seen as outsiders
- Police agencies are focused on publicity and getting the word out about their effectiveness at crime-fighting while intelligence work is focused on secrecy and never letting intelligence successes be known
- Police are taught that criminal justice record keeping should be clear and concise, with writing crisp and to the point, while there is no such thing as too much excess or irrelevant information for intelligence work
- Police are not equipped to deal with the kind of massive casualties that weapons of mass destruction can cause
- Police are not prepared to face a terrorist enemy who uses criminal means to obtain military objectives.[17]

While White may argue that the legal reform approach may be viable on the federal level, it would be far more difficult to implement, and understand, on the local level. Additionally, there is certainly not agreement at the leadership level of local law enforcement that today's Police Officer lacks the sophistication or intelligence to grasp these rather complex strategies.[18] While the following database approach may hold more promise for coordination and collaboration, there is surely a basis for legal reforms with an emphasis on intelligence gathering and dissemination.

[17] White, *Defending the Homeland*, 78.

[18] Personal interviews conducted with 243 California Police Chiefs and Sheriffs, 2004-2005.

D. DATABASE APPROACH

A third approach for law enforcement is the use of computer databases with regard to Homeland Security issues. The National Strategy for Homeland Security (2003) calls for connecting computer databases used in federal law enforcement, immigration, intelligence, public health surveillance, and emergency management. Further, DARPA's plan for Total Information Awareness is to merge some of these interconnections into a data mining system of systems involving the private sector, the finance/credit system, and the Internet.

Most of the databases involved would be government owned, where they are not so different from one another, and can probably be interconnected. Some, such as CDC's (Centers for Disease Control) epidemiology program, continuously scan disease patterns throughout the nation's healthcare system for signs of an outbreak. Others such as the Department of State's TIPOFF system compiles information on suspected terrorists collected by consular offices overseas and are already interconnected. There are large databases involved, two of the largest being those from Immigration (fugitive aliens alone number in the hundreds of thousands) and the FBI (NCIC, or the National Crime Information Center which tracks everything greater than a Class C misdemeanor and is already overburdened by the size of graphic files). To demonstrate the current law enforcement approach to database applications, the following is a partial list of government databases related to homeland security:

- AFIS- Fingerprint system to identify citizens
- CCD - Consolidated Consular Database, records of non-immigrant visa entries and exits
- CLASS - Consular Lookout and Support System; program for running background checks for visas
- CODIS - Combined DNA Index System used for solving crimes
- IBIS - Interagency Border Inspection System; immigration program used at ports of entry
- IDENT - Fingerprint system to identify aliens

- JITF-CT - Joint Intelligence Task Force Combating Terrorism, DIA database
- LEO - Law Enforcement Online; VPN with exclusive interactive briefings, alerts, and discussions
- NAILS - National Automated Immigration Lookout System
- NCIC - Contains criminal justice arrest records, fugitives, stolen property, and missing persons and items
- NDPIX - National Drug Pointer Index, DEA records of common targets in investigations
- NDSI - National Spatial Data Infrastructure, geo-mapping records with meta-data tags
- NIBIN - National Integrated Ballistics Information Network; unified ATF and FBI database, but mostly ATF
- NLETS - National Law Enforcement Telecommunication System, interstate license and registration records
- NSEERS - National Security Entry-Exit Registration System
- SEVIS - Student Exchange Visitor Information System, monitors foreign students
- TECS - Treasury Enforcement Communications System, for suspicious individuals and businesses
- TIPOFF - State Department program which searches for known and suspected terrorists
- TIPS - Terrorist Information and Prevention System, for anonymous tips

The problem with government databases is not with the federal government's attempt to integrate "watch lists," but at the state and local level. Some state and municipal police departments are as far behind as five years in such basic things as updating parking ticket records. In order to have a valid intelligence picture, a greater problem arises when one tries to integrate, or commingle, government databases with those in the private sector, such as credit card companies, e-commerce firms, or retailers.

For example, one would need about 15,000 fields just for merging the header (demographic) information across these databases, which would represent about 300,000 bytes per person. If you multiply this by 500 million people, the header records alone would require approximately 150,000,000,000,000 bytes (136 terabytes) and almost five years to stabilize. Then, there is the key identifier fields (also called crosswalk tables) which contain numerical records such as social security numbers or driver's license numbers which link the different databases together, and one of these has to be a unique identifier (pivot table) to put a workable interface on it.[19]

Since terrorists are likely to use fake IDs, a new unique identifier system may have to be developed, and this will require about ten years of data input time. Then, the transaction data is brought in, generally producing crashes and errors and generating the need for continual validation, duplication, and normalization. The computer database approach may be doable, but it will take years to perfect, huge improvements in technology, and something much faster than T1 Internet connections for law enforcement.

Secure intranets (on the .gov domain) and secure videoconferences will most likely remain the federal government's main way of information sharing with state and local governments, along with renaming the 93 Anti-Terrorist Task Forces (ATTFs) throughout the federal court districts into Homeland Security Task Forces (HSTFs). The ATTF/HSTF approach does not simply involve prosecutors, but Joint Terrorist Task Forces (JTTFs) (which have a longer history, going back to Chicago in the late 1970s) are a different thing. JTTFs now exist in all 56 FBI field offices where some elite state and local police are picked to be temporarily federalized. Since the powers of arrest are equalized, true, joint cooperation exists between the levels of government.

Aside from the dilemma of coordinating the myriad of databases, the collaboration required on the local level with regard to Homeland Security issues is enormous. The sheer dimension of the collaboration effort is overwhelming. Dr. William Pelfrey, in an unpublished Naval Postgraduate School paper, has listed the disparate disciplines associated with Homeland Security:

---

19 Government Security News, April 2004, 27.

- Law Enforcement
- Emergency Medical Service
- Fire
- Hazmat
- Emergency Dispatch
- Health Services
- Emergency Medical
- Elected officials
- Public Health
- Public Works
- Business Continuity
- Conveyances
- Cybersecurity and IT Infrastructure
- Educational Institutions
- Homeland Security
- Private Security
- Major Event Security
- Red Cross
- Public Information
- Media Management
- Private Sector
- Financial Institutions
- District Attorney
- Risk Management
- Skilled Trades
- Transportation Services
- Public/Private Utilities
- Military[20]

[20] William Pelfrey, Unpublished Paper, 2004.

Twenty-eight different disciplines that require coordination and collaboration. None of the current law enforcement or regional approaches addresses the coordination and collaboration that will be required to effectively address the homeland security issue on a local level. While collaboration may be more effective on a countywide basis, it still will require new structures, new agreements and most importantly, new leadership. Absent this leadership, no tactic or technology in homeland security will be sufficient.

E. LEADERSHIP

As an evolving reality, homeland security presents unique challenges for leaders: the context in which contemporary homeland security leaders operate is relatively new and it is rapidly changing and evolving. This requires that leaders be adaptable and flexible, acutely aware of the context in which they operate, with continual reevaluation in order to make sound decisions.

Effective leaders must establish direction and purpose, communicate that direction and purpose, and maintain the thrust of the group. They need to promote innovation and creativity and serve as a resource for invigorating the organizational culture. Leaders must also be resilient, maintain a multi-directional vision and focus, and develop an understanding of the psychological forces that move people. Only by doing these things can they make appropriate decisions about what to do and when to do it in a context full of conflicting data and opinions.

Homeland Security leaders have a critical role to play in developing strategy on all levels and promoting interagency collaboration, a critical element in achieving the strategy.

While there have been numerous studies conducted regarding leadership style and leadership models, I will review two specific models of leadership since I believe they hold the most promise for adaptation to the requirements facing law enforcement in 2005.

1. The Transactional vs. Transformational Leader

The transactional leader manages resources, tasks, and followers to accomplish a specific objective by balancing the concern for task with the concern for people. They are

managers who view their organizations as complicated machines and their employees as workforce. Workforces are managed by power and position.

Transformational leaders also manage resources, tasks, and followers to get a job done, but do it in an interactive way that enables others to perform to a higher standard. In the words of James MacGregor Burns, they "engage with others in such a way that leaders and followers raise one another to higher levels of motivation and morality."[21] Transforming leaders go beyond the boundaries of the current organizational system toward new possibilities that are rooted in shared values. By communicating shared values and visionary thinking, they partially transcend the structural barriers of manager/employee or political leader/citizen. These are charismatic leaders who supply vision, organization, and inspiration for their organizations.[22]

Numerous leadership studies have attempted to examine charismatic leadership categories more closely, focusing on the "transactional" and "transformational" approaches. In the early 1970s, Edwin P. Hollander, a professor of psychology at Baruch College, employed the term "idiosyncrasy credit" to stand for the freedom that members of a group were granted to act idiosyncratically. He showed that a seeming paradox existed: Giving followers a measure of autonomy increased their willingness to respond to a leader's directions. [23]

Burns crystallized the stress on transformational and transactional styles. His massive study “Leadership” has, in fact, become the Rosetta stone of recent leadership studies. Drawing on a wide range of historical examples and figures, from William Lloyd Garrison to Sir Robert Peel to Franklin Roosevelt, Burns offered an ambitious review on the nature of leadership, one that returned to Weber's and Simmel's emphasis on the leader-follower nexus. Unquestionably, Burns's most important insight was to draw a distinction between transformational and transactional leadership. Where transactional leadership is merely a version of management that appeals to the self-interest of followers, transformational leadership alters the expectations of followers. With integrity

---

[21] James McGregor Burns, *Leadership* (New York: Harper and Row, 1978), Chapter 3.

[22] Bernard Bass, *Transformational Leadership* (New York: Lawrence Erlbaum and Assoc., 1997), Chapter 2.

[23] Edwin Hollander, *The Balance of Leadership and Followership (*University of Maryland, Academy of Leadership Press, 1997), http://www.academy.umd.edu/publications/klspdocs/follower_intro.htm.

in leadership an essential prerequisite and like Simmel and Weber, Burns contends that leaders can elevate their followers to new levels of morality and rectitude: "Moral leadership emerges from, and always returns to, the fundamental wants and needs, aspirations and values of followers."[24]

In an attempt to refine further the understanding of transformational leadership, Marshall Sashkin, an adjunct professor at George Washington University, has devised a "Visionary Leadership Theory" to take account not only of the practices of leaders but also of the effect of their behavior on the culture of an organization. Sashkin argues that followers are transformed because they internalize the values of the organization.[25] The task of the leader is to disseminate the organizations principles and to enunciate the values that animate the organization. The ultimate paradox, Sashkin finds, is that the effective transformational leader can employ a managerial approach in order to transform his followers. I would argue that this is the essential ingredient required for the development of the law enforcement role in homeland security.

Perhaps the most successful promoter of the transformational model in the business world is Warren Bennis, professor of management at the University of Southern California. Former Vice President Albert Gore reportedly made Bennis's “On Becoming a Leader” (1989) recommended reading for his advisers. Blunt in manner, Bennis decries "management education" and calls for the training of leaders. "Leaders conquer the context ... while managers surrender to it," he says.[26]

Transformational leadership does not derive merely from the attributes of great leaders. It is the joint production of a team having multiple leaders. It develops as an interactive process between leaders and followers. Its driving force is "intended real change" rather than simply the leader's vision. The motivations of leadership are jointly developed "mutual purposes" rather than a leader's exhortation calling followers to a higher ground.

In this process, organizational managers become transforming leaders with important new systemic responsibilities. They combine the role of process designer with that of administrator. They become promoters of an organizational culture that initiates

[24] Burns, *Leadership*, Chapter 3.

[25] Marshall Sashkin, *The Visionary Leader* (Bristol, CT: New World Press, 1998), Chapter 1.

[26] Warren Bennis, *On Becoming a Leader* (Reading, MA: Perseus Publishing, 1994), 4.

and sustains the transformational leadership process. They instigate and maintain a process of group learning and face formidable challenges in trying to reach the level of consensual decision-making.

While these two forms of leadership should be present in the Homeland Security effort, there is a great need for transformative leaders. Despite the challenges inherent in transformational leadership, local law enforcement can also be implementing it because it is ideally suited for dealing with unpredictable and chaotic change.

In my discussions with the California Law Enforcement officials, every one acknowledged the need for a transformational style, yet each acknowledged that they rarely used that model. It is somewhat ironic that unless law enforcement leaders adopt this style with regard to information sharing and intelligence dissemination, the counter-terrorism effort will be for naught.

It is no mystery that different times call for different kinds of leaders. In the business world, patient, low-profile managers are sometimes preferable to forceful visionaries. The energetic Lee Iacocca functioned best when he was leading Chrysler out of financial disarray. A similar rule exists in the world of politics. Winston Churchill was ejected from office once he had fulfilled his mission of winning World War II. Leaders, of course, are usually incapable of reconciling themselves to the fact that they can leave an imprint only when a certain constellation of historical forces is present. After a friend commiserated with Churchill and told him his defeat at the polls was a blessing in disguise, Churchill muttered, "If it is, the disguise is perfect." Again, the requirement for transformational leadership in the law enforcement arena is reinforced.

Evidence supporting the transactional -- transformational leadership paradigm has been gathered from all continents except Antarctica -- even offshore in the North Sea. The transactional -- transformational paradigm views leadership as either a matter of contingent reinforcement of followers by a transactional leader or the moving of followers beyond their self-interests for the good of the group, organization, or society by a transformational leader. The paradigm is sufficiently broad to provide a basis for measurement and understanding that is as universal as the concept of leadership itself.

Numerous investigations (field studies, case histories, management games, interviews, and laboratory studies) point to the robustness of the effects of transformational and charismatic leadership.[27]

To date, the study of leadership has successfully identified many important traits of leaders and made valuable contributions to our understanding of how leaders and followers in organizations interact.

The homeland security concerns we face in law enforcement in 2005 demand just such an approach - transformational leadership and a different form of collaboration and cooperation than we have traditionally experienced in the law enforcement field. The question that requires an answer is whether law enforcement has a clearly defined approach and if they do, how to best implement it. While the issue of regionalization may answer the "how" question, local law enforcement, using a transformational leadership model, must first address their fundamental role and how to accomplish that task.

In summary, I believe that the leadership required must coalesce with the desired approach of law enforcement. There are many reasons to believe that a networked, transformational leadership style, coupled with database linkages, may be the best method. While I have merely touched on a new leadership model and the role of law enforcement, I would suggest, based upon the view of the Police Chiefs and Sheriffs of California, that future study might indicate a regional (county by county) approach may offer the best opportunity for implementation.

If transformational leadership emerges, success and effectiveness will depend to some extent on the environment, the organizations involved, the tasks and goals delineated, and the distribution of power.

Since the attacks of September 11, 2001, the United States has made significant strides toward strengthening homeland defense, improving emergency response, and reducing community fear. Agencies at the federal, state, and local levels are beginning to create positive working relationships with each other and to integrate their strategies for responding to the threat of terrorism. They are recognizing not only the importance, but also the need for enhanced vertical and horizontal communications.

27. Bernard M. Bass, "Does the Transactional -- Transformational Leadership Paradigm Transcend Organizational and National Boundaries?" *American Psychologist* 52, no. 2 (1997): 130.

Law enforcement agencies have historically been charged with preserving the safety and security of the public. Regrettably, this mission is no longer limited to traditional crime—the prevention and deterrence of another terrorist attack on American soil have become a crucial part of this mission, leaving law enforcement agencies at every level of government responsible for restoring and maintaining a public sense of security.

How can law enforcement fulfill this new obligation successfully? What is the key to maximizing the probability of success in thwarting the next terrorist attack? The answer lies in the ability to know as much as possible about the threat in order to respond accordingly and efficiently. The answer is the use of reliable intelligence.

Identifying when, where, and how a terrorist attack will happen is tremendously difficult at best, but absolutely critical because that knowledge could save hundreds or maybe thousands of American lives. The most effective weapon in the war on terrorism is intelligence - the detailed analysis, evaluation, and interpretation of information. The nucleus of this weapon is information collected and shared by federal, state, and local law enforcement agencies.

Intelligence begins as bits of raw information or data. Information becomes intelligence when it is organized, analyzed, and interpreted with a specific focus. Without intelligence, agencies may be less than prepared to make the strategic and tactical decisions necessary to prevent and respond to critical incidents. This concept applies to both criminal and terrorist investigations.

The primary challenge for local law enforcement is understanding through data analysis and then utilizing, through leadership, intelligence in a community policing context. Before information becomes intelligence, numerous questions must be answered.

What information should be collected?

How will it be analyzed and by whom?

What information must be shared and what information must be kept confidential?

How can information on individuals be collected without jeopardizing their rights as American citizens?

These are just some of the issues that must be addressed before good information can become useful intelligence. Yet the preceding questions cannot be answered apart from an examination of intelligence analysis itself. It is only with a clear comprehension of the analytic process that one can fully explore the subsequent collection and sharing aspects of the intelligence function. Identifying the central elements of a successful intelligence function will enable law enforcement agencies to generate practical solutions to the aforementioned challenges, establish rewarding intelligence functions specific to their needs, develop protocols for working with the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) and other federal agencies and eliminate barriers to sharing intelligence.

III. EXISTING ARRANGEMENTS

While discussions of information sharing frequently focus on how technology can be used to break down the so-called "stove pipes" that purportedly inhibit collaboration among government agencies, it is important to recognize that these initiatives are more than simply information technology projects. Instead, they represent a specific component of ongoing efforts to improve the management, efficiency, and efficacy of government information resources, often associated with electronic government or e-government. As such, information sharing initiatives are characterized by their programmatic elements as well as their technology elements.

Some of the most common categories or types of information being shared through these initiatives include intelligence, homeland security, law enforcement, and critical infrastructure information. Information shared and technology used by these initiatives can vary widely. However, an overarching purpose of most of these initiatives is to facilitate better collaboration and information analysis through the use of improved information technology and the development of common information standards.

Concerns about coordination and duplication of these initiatives have been raised since there currently appears to be no centralized inventory of all the information sharing initiatives being carried out within and between the federal, state, and/or local levels. GAO has reported, however, that efforts to fight terrorism have spurred the growth of the number of initiatives at all levels of government since the September 11, 2001, attacks. Three existing information sharing initiatives are discussed below to provide general examples of how information sharing is sometimes carried out. They also provide a roadmap of sorts, by which federal, state and local agencies may refine and focus their intelligence sharing efforts.

A. JOINT REGIONAL INFORMATION EXCHANGE SYSTEM (JRIES) AND THE HOMELAND SECURITY INFORMATION NETWORK (HSIN).

In December 2002, JRIES began as a pilot project for the sharing of counterterrorism information between local and state law enforcement and the

Department of Defense (DOD). JRIES was initiated by the Joint Intelligence Task Force - Combating Terrorism (JITF-CT), led by the Defense Intelligence Agency (DIA). The initial participants included the New York Police Department Counterterrorism Bureau (NYPD-CTB) and the California Department of Justice Anti-Terrorism Information Center (CATIC). After assessment of the pilot phase, JRIES became operational in February 2003. The number of participants has also grown to include other municipalities, states, and federal agencies.[28]

In February 2004, the Department of Homeland Security (DHS) announced the launch of its Homeland Security Information Network (HSIN) initiative, designed to connect all 50 states, five U.S. territories, and 50 major urban areas with the Homeland Security Operations Center (HSOC) at the department. To accomplish this goal, DHS adopted the JRIES infrastructure, expanding both its capabilities and its community of users beyond its original "law enforcement and intelligence counterterrorism mission" while leaving the original JRIES system in place.[29] In July 2004, DHS announced that it achieved connectivity to all 50 states.[30] JRIES/HSIN is anticipated to eventually include users such as state homeland security advisers, state adjutant generals (National Guard), state emergency operations centers, local emergency services (fire, police, and other first responders), and possibly private sector actors as well. A significant focus of the expanded JRIES/HSIN network will be to prevent terrorist attacks by capitalizing on the existing human and information resources at the federal, state, and local levels, and enabling the real time collaboration and exchange of information for improved awareness and quicker response to threats.[31]

Some civil liberties organizations have raised concerns regarding the exchange of information by state and local law enforcement agencies with DIA, an intelligence agency barred from collecting information domestically. Concerns also have been raised

---

[28] U.S. Department of Justice, Office of Justice Programs, *The National Criminal Intelligence Sharing Plan (*Washington, October 2003), 45-56.

[29] U.S. Department of Homeland Security, "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities," Press Release, Feb. 24, 2004.

[30] Dibya Sarkar, "HSIN Starts Five Months Early," *Federal Computer Week,* July 8, 2004.

[31] U.S. Department of Homeland Security, op. cit.

about the potential collection information regarding the activities of legitimate political or social organizations, such as anti-war groups.[32]

JRIES functions as a secure virtual private network (VPN), connecting various participant data sources using encrypted communications via the Internet. JRIES relies upon commercial, off-the-shelf technology and Web-based software that enables users to access database and analysis applications, send secure e-mail, send and receive maps and other graphics, and collaborate in real time online.[33]

JRIES/HSIN is currently used to exchange so-called sensitive but unclassified (SBU) information, although DHS plans to upgrade the security of the network to allow for the exchange of security classified information at the "Secret" level by fall 2005.

In the future, DHS also plans to develop an interface between JRIES and RISSNET, a long established nationwide network of criminal databases used by law enforcement agencies.[34]

On July 20, 2005, Matthew Broderick, director of the Homeland Security Operations Center said in testimony to the House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, that "The Homeland Security Information Network-Secret is an immediate, inexpensive and temporary approach to reach state and local homeland security and law enforcement sites that can receive secret-level information, the new network is operating and will continue to do so until the DHS secret-level backbone called the Homeland Security Data Network is initiated in fiscal 2007."[35]

B. REGIONAL INFORMATION SHARING SYSTEM (RISS) PROGRAM.

The RISS Program is an established system of six regional centers that are used to "share" intelligence and coordinate efforts against criminal networks that operate in many

---

[32] Justin Rood, "Pentagon Has Access to Local Police Intelligence Through Office in Homeland Security Department," *CQ Homeland Security*, July 6, 2004.

[33] Brian Robinson, "DHS Unfolds Safety Net," *Federal Computer Week*, June 21, 2004.

[34] U.S. Department of Homeland Security, op. cit.

[35] Government Computer News, July 22, 2005.

locations across jurisdictional lines.[36] The RISS Program was created to combat traditional law enforcement targets, such as drug trafficking and violent crime, but has been expanded to include other activities, such as terrorism and cyber-crime.

According to its website, RISS has "member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England."[37] The RISS program uses a regional approach, so that each center can tailor its resources and focus on the specific needs of its area, while still coordinating and sharing information as one body for national-scope issues.[38] The origins of the RISS Program date to 1974, when the Department of Justice awarded its first grant to allow police departments in the southern U.S. to share/exchange information with each other via computers.[39] This support helped create the first of the six regional centers, the Regional Organized Crime Information Center (ROCIC).[40] The other regional centers include the Rocky Mountain Information Network (RMIN),[41] the New England State Police Information Network (NESPIN),[42] the Mid-States Organized Crime Information Center (MOCIC),[43] the Western States Information Network (WSIN),[44] and the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN).[45]

Membership in each of the centers includes federal, state, and local law enforcement agencies, for an estimated total of "nearly 7,000 law enforcement and criminal justice agencies representing over 700,000 sworn officers."[46] The RISS Program continues to be federally funded through the Bureau of Justice Assistance (BJA) at the Department of Justice (DOJ), which also has program management oversight

---

[36] For a detailed description of RISS, see (http://www.iir.com/riss/ and http://www.rissinfo.com/).

[37] Available at (http://www.iir.com/riss/).

[38] See (http://www.rissinfo.com/).

[39] U.S. Department of Justice, Bureau of Justice Assistance, "Regional Information Sharing Program," *Bureau of Justice Assistance Program Brief* (Washington, April 2002).

[40] Includes 14 regional member states.

[41] Includes eight western states.

[42] Includes six New England states.

[43] Includes nine mid-west states.

[44] Includes five western states, including California.

[45] Includes nine Eastern states.

[46] See (http://www.rissinfo.com/overview2.htp).

responsibilities. In addition, RISS centers are required to be in compliance with Criminal Intelligence Systems Operating Policies regarding the confidentiality of information collected and shared.[47] Each of the six RISS centers provide its member agencies with a range of services, including:

- Information sharing — primarily through the operation of the RISS secure intranet (RISSNET), providing secure databases and investigative tools.
- Analysis — including the preparation of analytical products, compilation and analysis of data, and computer forensics analysis.
- Equipment loans — inventories of specialized investigative and surveillance equipment, including photographic, communications, and surveillance equipment, for member agencies to borrow for multi-jurisdictional investigations.
- Confidential funds — following federal and center guidelines, money that can be used to purchase information, contraband, stolen property, and other evidentiary items, as well as to pay investigative expenses for multi-jurisdictional investigations.
- Training — meetings and conferences for training on information sharing techniques, anti-terrorism training; and training in surveillance techniques, equipment use, safety, and analysis techniques.
- Technical assistance — training and assistance for activities such as requesting analytical services, and RISSNET installation and support.[48]

The centerpiece of the RISS Program information sharing activities is a secure intranet, RISSNET, which is capable of sharing electronically what is termed "sensitive but unclassified information." RISSNET participants can either connect a single computer to the intranet, or establish a node connection, enabling wider access through their agency's network. RISSNET participants use a virtual private network (VPN) connection over the Internet to access the RISSNET gateway firewall, whereupon the user's identity is authenticated and access is granted to the secure intranet. The secure

[47] See CFR Part 23; U.S. Department of Justice, op. cit.

[48] See (http://www.rissinfo.com/services.htm).

intranet is a dedicated network carried over frame relay circuits (a guaranteed amount of bandwidth carried over public telephone lines) connecting the RISS centers to the database resources. Security is maintained through the use of encryption, smart cards, and other Internet security protocols.[49]

This system enables participants to send and receive secure e-mail transmissions with other RISSNET participants, as well as use secure Web browser sessions to access data. RISSNET also provides access to a number of other resources, including:

- **RISS center websites** — each of the six RISS centers has a website that provides information on its services and resources, and provides access to criminal intelligence databases.
- **RISSIntel/RISSNET II** — electronically linked collection of web-based criminal intelligence databases with information provided by member agencies.
- **RISSGang** — the RISS National Gang Database, a crime-specific database related to gangs and gang members, including both text information and images, such as photographs, gang tattoos, and gang graffiti.
- **RISSLeads** — the RISS Investigative Leads Bulletin Board, a newsgroup server where participants can post case-related information for the purpose of generating investigative leads and can exchange information with other participants.
- **RISSSearch** — a search engine that identifies and retrieves data from multiple databases and information sources, including restricted information sites, sensitive but unclassified sites, and public Internet sites.
- **RISSTraining** — electronic resources for anti-terrorism training.
- **RISSLinks** — a data visualization tool for analyzing and showing associations among the results from multiple databases.

[49] U.S. Department of Justice, op. cit.

- **RISSLive** — an online, real-time communications medium to facilitate real-time information sharing among participants.[50]

Another recently developed resource is the RISS Anti-Terrorism Information Exchange (ATIX). Initiated in late 2002, RISS ATIX represents an expansion of the efforts to facilitate communication and information sharing among personnel responsible for planning and implementing actions to prevent, mitigate, and recover from terrorist incidents and disasters. RISS ATIX participants include constituencies that have not traditionally participated in RISS. RISS ATIX participants include both government and private sector participants, who are divided into ATIX communities, based on their functions.[51]

According to the RISS ATIX website, some of the ATIX communities include "state, county, local, tribal, and federal government; law enforcement; emergency management; disaster relief; utilities; and, among others, the chemical, transportation, and telecommunication industries."[52] Since becoming operational, RISS ATIX has been used to facilitate communications for events such as Hurricane Isabel in September 2003, the G8 Summit at Sea Island, Georgia, in June 2004, and both the Republican and Democratic national conventions in summer 2004.[53]

RISS ATIX utilizes four primary components to facilitate communication and information sharing. These include:

- **RISS ATIX Web page** — news articles, online resources, and contact information tailored to the various ATIX communities.
- **RISS ATIX bulletin board** — a newsgroup server where participants can post information related to terrorism, disasters, and homeland security, as well as "page" online participants and send secure e-mail messages.

---

[50] National Narcotic Officers' Association Coalition, "Regional Information Sharing Program," *NNOAC Insight*, April 2005, 33.

[51] "The RISS Program", 2002.

[52] See http://www.rissinfo.com/rissatix.htm, February, 2005.

[53] Michael Lynch, "Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State, Local Governments," Senate hearing statement, March 23, 2005.

- **ATIXLive** — an online, real-time communications medium to facilitate real-time information sharing among participants, including the "paging" function and the ability to send secure e-mail messages from within the ATIXLive application.
- **ATIX secure e-mail** — a secure e-mail application to send and receive homeland security alerts and exchange information with other participants.[54]

On September 1, 2002, RISSNET interconnected with the FBI Law Enforcement Online (LEO) system to create a so-called "virtual single system" for the purpose of exchanging sensitive but unclassified homeland security information. Both RISSNET and LEO participants can access these resources combined using a single logon identifier. Participants can also exchange secure e-mail messages. RISSNET has established, or is in the process of establishing, interconnections with other information sharing networks as well, including the National Law Enforcement Telecommunications System (NLETS), the Criminal Information Sharing Alliance (CISAnet), and the subsequently failed, Multi-state Anti-Terrorism Information Exchange (MATRIX) Pilot Project.[55] As with other information sharing initiatives, civil liberties organizations have raised concerns about privacy and the potential misuse of personal data as more information sources become interconnected and available to a larger number of users.

C. MULTI-STATE ANTI-TERRORISM INFORMATION EXCHANGE (MATRIX) PILOT INFORMATION SHARING PROJECT.

The MATRIX project was initially developed in the days following the September 11, 2001, terrorist attacks by Seisint, a Floridabased information products company, in an effort to facilitate collaborative information sharing and factual data analysis. At the outset of the project, MATRIX included a component Seisint called the

54 See http://www.rissinfo.com/rissatix.htm, March 2005.

55 "The RISS Program." 2002.

High Terrorist Factor (HTF), which was designed to identify individuals with high HTF scores, or so-called terrorism quotients, based on an analysis of demographic and behavioral data.

Although the HTF scoring system appeared to attract the interest of officials, this feature was reportedly dropped from MATRIX because it relied on intelligence data not normally available to the law enforcement community and because of concerns about privacy abuses.[56]

In initial form, the MATRIX pilot project was administered through a collaborative effort between Seisint, the Florida Department of Law Enforcement (FDLE)[57], and the Institute for Intergovernmental Research (IIR), a "Florida-based nonprofit research and training organization, [that] specializes in law enforcement, juvenile justice, and criminal justice issues."[58] FDLE served as the "security agent" for MATRIX, administering control over which agencies and individuals had access to the system. FDLE was also a participant state in MATRIX. IIR was responsible for administrative support, and was the grantee for federal funds received for MATRIX.[59]

Before closing, it had been reported that the MATRIX pilot project had received a total of $12 million in federal funding — $8 million from the Office for Domestic Preparedness (ODP) at the Department of Homeland Security (DHS), and $4 million, from the Bureau of Justice Assistance (BJA) at the Department of Justice (DOJ).[60]

The analytical core of the MATRIX pilot project was an application called Factual Analysis Criminal Threat Solution (FACTS), described as a "technological, investigative tool allowing query-based searches of available state and public records in the data reference repository."[61] The FACTS application allowed an authorized user to search "dynamically combined records from disparate datasets" based on partial

---

[56] Brian Bergstein, "Database Firm Tagged 120,000 Terrorism "suspects" for Feds," (Biloxi, MS) *Sun-Herald*, May 20, 2004.

[57] The FDLE website is available at (http://www.fdle.state.fl.us/), March 2005.

[58] The IIR website is available at (http://www.iir.com/), March 2005.

[59] See (http://www.matrix-at.org/roles.htm), March 2005.

[60] John Schwartz, "Privacy Fears Erode Support for a Network to Fight Crime," *New York Times*, March 15, 2004.

[61] For a more detailed description of FACT, see (http://www.matrix-at.org/FACTS_defined.htm), March 2005.

information that could "assemble" the results.[62] The data reference repository used with FACTS represented an amalgamation of over 3.9 billion public records collected from thousands of sources.[63]

The data contained in FACTS included FAA pilot license and aircraft ownership records, property ownership records, information on vessels registered with the Coast Guard, state sexual offender lists, federal terrorist watch lists, corporation filings, Uniform Commercial Code filings, bankruptcy filings, state-issued professional license records, criminal history information, department of corrections information and photo images, driver's license information and photo images, motor vehicle registration information, and information from commercial sources that "were generally available to the public or legally permissible under federal law."[64]

The data reference repository was said to exclude data such as telemarketing call lists; direct mail mailing lists; airline reservations or travel records, frequent flyer/hotel stay program membership information or activity; magazine subscription records; information about purchases made at retailers or over the Internet; telephone calling logs or records; credit or debit card numbers; mortgage or car payment information; bank account numbers or balance information; records of birth certificates, marriage licenses, and divorce decrees; and utility bill payment information. Participating law enforcement agencies utilized this information sharing and data mining resource over the Regional Information Sharing Systems (RISS) secure intranet (RISSNET), described above.

Some civil liberties organizations raised concerns about law enforcement actions being taken based on algorithms and analytical criteria developed by a private corporation — in this case, Seisint — without any public or legislative input.[65]

---

[62] For a more detailed description of FACT, see (http://www.matrix-at.org/FACTS_defined.htm), March 2005.

[63] See (http://www.matrix-at.org/newsletter.pdf), March 2005.

[64] For more information about data included in and excluded from the data reference repository, see (http://www.matrix-at.org/data_sources.htm), March 2005.

[65] William Welsh, "Feds Offer to Mend Matrix," *Washington Technology* May 24, 2004.

Questions were also raised about the level of involvement of the federal government, particularly the Department of Homeland Security and the Department of Justice, in a project that was ostensibly focused on supporting state-based information sharing.[66]

From initiation, the MATRIX pilot project suffered setbacks in recruiting states to participate. The lack of participation was especially troubling for a networked information sharing project such as MATRIX because, as Metcalfe's Law suggests, "the power of the network increases exponentially by the number of computers connected to it."[67] While as many as 16 states had been reported to have either participated or seriously considered participating in MATRIX at its outset, several chose to withdraw, leaving a current total of five states, including Florida, Michigan, Ohio, Pennsylvania, and Connecticut, actively participating. State officials have cited a variety of reasons for not participating in MATRIX, including costs, concerns about violating state privacy laws, and duplication of existing resources.[68]

To help address the privacy concerns associated with a centralized data repository, some officials have suggested switching to a distributed approach whereby each state would maintain possession of its data and control access according to its individual laws.

In June 2005, the MATRIX project was abandoned and all states withdrew.

---

[66] Robert O'Harrow, Jr., "Anti-Terror Database Got Show at White House," *Washington Post*, May 21, 2004.

[67] For a more detailed description of Metcalfe's Law, see (http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214115,00.html), March 2005.

[68] The states that have decided to withdraw from the project include Alabama, California, Georgia, Kentucky, Louisiana, New York, Oregon, South Carolina, Texas, Utah and Wisconsin.

THIS PAGE LEFT INTENTIONALLY BLANK

IV. LOS ANGELES TERRORISM EARLY WARNING GROUP

The concept is simple. Representatives of various first-responder agencies in a given area agree to meet on a regular basis to share information, analyze potential threats, plan for emergency procedures and establish the various chains of command and communication in the event of an attack.

"Because they are looking at threats, they can help direct preparedness," says Brian Houghton, Director of Research for the National Memorial Institute for the Prevention of Terrorism, in Oklahoma City. "Having people looking at what the threats are, they can more effectively utilize funding, as opposed to just building a wish list from the most vocal departments."[69]

The Los Angeles County Terrorism Early Warning (TEW) Group is the paradigm for such groups, partly because they have been at it longer than anyone else in the nation and they are the largest group, with about two dozen full-time staff members. The Los Angeles TEW was established in 1996 to perform as an interagency information sharing and analysis function designed to serve the information needs of local, state, and federal agencies involved in all phases of homeland security operations.

With an early attempt at transformational leadership and integration of disparate databases and agencies, the LA group may be the shining example of the future of law enforcement anti-terrorism efforts. While the measurements of success, the number of "preventions," are very difficult to count, the joint effort approach certainly puts everyone on the same page. As the Deputy Commissioner for Intelligence at NYPD, David Cohen, said, "I don't know what we've stopped, it's impossible to calculate, and I don't spend much time thinking about it. I have to be thinking about the next thing."[70]

---

[69] Brian Houghton (Director of Research for the National Memorial Institute for the Prevention of Terrorism), interview with Author, March 2005.

[70] David Cohen (New York Police Department Deputy Commissioner), CNN interview, April 2005.

What follows is a brief look at the Los Angeles TEW and the possible model for other efforts. There are approximately 14 similar type groups operating across the country.[71]

A. THE TEW MODEL

The TEW is a multilateral, multi-jurisdictional, and multi-disciplinary effort. It integrates law enforcement, fire, health, and emergency management agencies to address the intelligence needs for combating terrorism and protecting critical infrastructure. The TEW goes beyond criminal intelligence fusion and analysis. It results in "all source/all phase" fusion. In other words, it integrates all the information necessary for achieving a situational understanding at all phases of operations (before, during, and after an incident).

The TEW in Los Angeles includes a multidisciplinary fusion center staffed by "core agencies" including the Los Angeles County Sheriff's Department, Los Angeles Police Department, Los Angeles Division of the FBI, Los Angeles Fire Department, Los Angeles County Fire Department, and Los Angeles County Health Department. The TEW also receives support from state agencies and independent police, fire, and health agencies in Los Angeles County. The core agencies contribute permanent and surge staff, forward all potential terrorist criminal leads and pre-incident indicators to the TEW for assessment, and participate in joint training and exercises to facilitate TEW operations. In addition, each agency (and stations or units at larger agencies) have established Terrorism Liaison Officers (TLOs) to enhance two-way information exchange between the TEW and cooperating agencies. The TEW works in cooperation with Joint Terrorism Task Forces and other investigative agencies to improve prevention and response and to ensure an appropriate exchange of information between investigative and response entities.

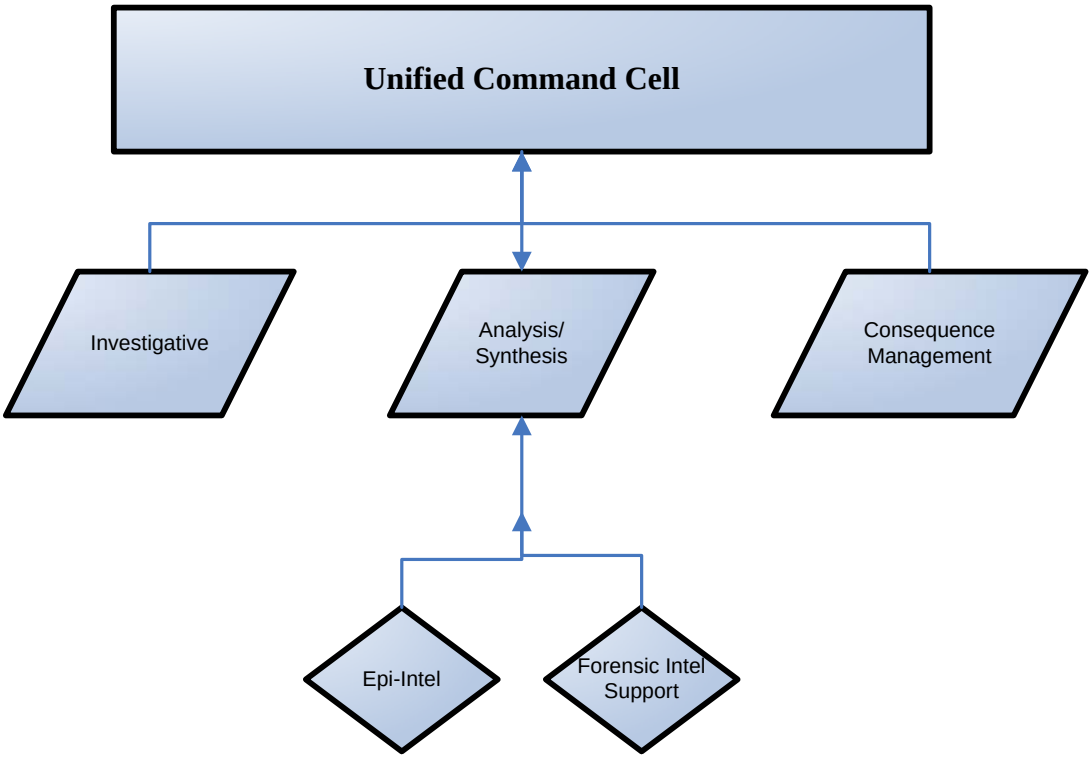
[71] The following cities/counties have established a TEW or similar group: San Diego, Los Angeles County, Inland Empire (San Bernardino County), Sacramento, Pierce County Washington, Albuquerque, Tulsa, New Orleans, Minneapolis/St. Paul, Cincinnati, Miami, Phoenix, Detroit and Denver. (From an informal survey conducted by the National Tactical Officers Association, 2005).

B. TEW ORGANIZATION

As depicted in Figure 1, the TEW is organized into six mutually supportive cells. The responsibilities of each cell are described below:

- The Unified Command cell provides direction, sets intelligence requirements, and interacts with the incident command entities.
- The Analysis/Synthesis cell coordinates net assessment activities and develops the collection plan. (It requests information be sought by the various net assessment elements and develops the results of all the cells' analysis into actionable intelligence products, including advisories, alerts, warnings, and mission folders to assist response.)
- The Consequence Management cell assesses the law enforcement, fire, and health consequences of the event.
- The Investigative Liaison cell coordinates with criminal investigative entities and the traditional intelligence community.
- The Epidemiological Intelligence (Epi-Intel) cell is responsible for real-time disease surveillance and coordination with the disease investigation.
- The Forensic Intelligence Support cell exploits a range of technical means to support the TEW fusion process. These include chemical, biological, radiological, and nuclear explosives (CBRNE) reconnaissance, the use of sensors and detectors, and geospatial tools (such as mapping, imagery, and GIS products).

Figure 1. – TEW Net Assessment Organization



The Terrorism Early Warning (TEW) Group model is designed for both "first responder" agencies and "follow-on" response agencies, as a cooperative vehicle for obtaining and assessing the information and intelligence needed for an effective homeland security response. It establishes a high degree of interoperability among levels of responders (local, state, federal), disciplines (law enforcement, fire service, public health and medical), and civil and military agencies. This model demonstrates that intelligence is an important element in forging an interagency response.[72]

The Appendix is a Ventura Police Department Training Bulletin that describes another recent effort toward Information and Intelligence sharing initiated by the State of California.

[72] Sgt. John Sullivan, Los Angeles County Sheriff's Department, and Commander Mike Grossman, Los Angeles County Sheriff's Department, NPS Presentation, January, 2005.

V. CALIFORNIA LAW ENFORCEMENT LEADERSHIP PERSPECTIVE

From 2004 through 2005, I spoke with 243 Police Chiefs and Sheriffs in California. In asking a series of basic questions, I believe their answers are indicative of the current state of intelligence and information sharing at the local level. As a result of the information obtained during these interviews, I combined their responses with the existing information available to draw several conclusions as to the next steps in this information sharing journey that we began on September 11, 2001.

Since the role of law enforcement agencies varies according to Department size, I have grouped the Departments into the following categories:

Group One – Over 500 sworn Officers

Group Two – 100-500 Sworn Officers

Group Three – 50-100 Sworn Officers

Group Four – Less than 50 Sworn Officers

Table 1. Responses to Interview Questions, Group 1 (Over 500)

N = 12

Question	Yes	No
Is there adequate information/intelligence sharing between federal, state and local agencies?	17%	83%
Do you have adequate resources to accomplish your intelligence collection responsibility since September 11?	0%	100%
Has your agency received adequate training in intelligence/information sharing requirements?	75%	25%
Are you aware of the variety of federal databases and information sharing technologies?	83%	17%

Do you receive daily, updated intelligence briefings?	100%	0%
Would you participate in a fusion center in your county?	92%	8%

Table 2. Responses to Interview Questions, Group 2 (100-500)
N=45

Question	Yes	No
Is there adequate information/intelligence sharing between federal, state and local agencies?	22%	78%
Do you have adequate resources to accomplish your intelligence collection responsibility since September 11?	13%	87%
Has your agency received adequate training in intelligence/information sharing requirements?	13%	87%
Are you aware of the variety of federal databases and information sharing technologies?	62%	38%
Do you receive daily, updated intelligence briefings?	31%	69%
Would you participate in a fusion center in your county?	89%	11%

Table 3. Responses to Interview Questions, Group 3 (50-100)
N=74

Question	Yes	No
Is there adequate information/intelligence sharing between federal, state and local agencies?	19%	81%
Do you have adequate resources to accomplish your intelligence collection responsibility since September 11?	11%	89%

Has your agency received adequate training in intelligence/information sharing requirements?	5%	95%
Are you aware of the variety of federal databases and information sharing technologies?	27%	73%
Do you receive daily, updated intelligence briefings?	27%	73%
Would you participate in a fusion center in your county?	88%	12%

Table 4. Responses to Interview Questions, Group 4 (<50) N=112

Question	Yes	No
Is there adequate information/intelligence sharing between federal, state and local agencies?	29%	71%
Do you have adequate resources to accomplish your intelligence collection responsibility since September 11?	12%	88%
Has your agency received adequate training in intelligence/information sharing requirements?	10%	90%
Are you aware of the variety of federal databases and information sharing technologies?	28%	72%
Do you receive daily, updated intelligence briefings?	12%	88%
Would you participate in a fusion center in your county?	75%	25%

The survey results are only meant to indicate the current state of law enforcement in California with regard to homeland security issues and information sharing. It is reassuring to know that the overwhelming majority of large agencies (over 500 sworn) feel that they have received adequate training, are aware of the variety of databases available, receive daily intelligence briefings and would (or do) participate in a local

fusion center effort. It is also noteworthy that the main difference in the responses by department size is in the area of daily counter-terrorism intelligence briefings. Only the largest agencies seem to have a consistent approach in that regard.

It is also very clear that, across the board, local law enforcement agencies feel that there is inadequate information sharing and resources available to accomplish the homeland security mission. While the term adequate is open to a variety of interpretations, the context of the discussion and subsequent question for the Chiefs and Sheriffs dealt essentially with timeliness and complete information.

An excerpt from an article in the New York Times, July 29, 2005 states, "Among the leaders is William J. Bratton, the Los Angeles Police Chief, who said in interviews Wednesday and Thursday that while the quality of information from the F.B.I. and the Department of Homeland Security was generally good, it often arrived far too late to be of any immediate value to local police departments."

"The frustration is that intelligence gathering and sharing networks at the federal level are not working for local chiefs of police," Chief Bratton said. "We're used to things breaking very quickly and have to respond quickly. We don't have the luxury of waiting."

He said the federal agencies and joint terrorism task forces that include local officials were chiefly investigative and analytical agencies and were not geared to providing real-time intelligence to local police. Local police and sheriffs departments, not federal authorities, have to decide quickly how to deploy their troops to respond to an immediate threat or an incident like the London subway bombings this month."[73]

The idea of a joint partnership and shared information is voiced repeatedly by California law enforcement executives. It is best summarized by the following statements made by the two Chief's from mid-size California law enforcement agencies:

> Local law enforcement is not 100% correct. We all have to meet half way. There has to be an assessment of threats and a value judgment. But the federal government has to trust local officials to work with INS, DHS, FBI, in joint assessments. We're ignored in our assessment of things. The federal government must be more flexible.

[73] John Broder, "Police Chiefs Moving to Share Terror Data," *New York Times*, July 29, 2005.

Real intervention is a partnership that's horizontal and vertical. We cannot have a clear understanding of how terrorists function if we do not take into account the local police. We have to bring forth a new concept of prevention – we don't have that curriculum. All tools now rest with the federal government, but their knowledge is disassembled. Even the JTTFs don't have the picture. We must socialize the sharing of resources, including intelligence. And we should audit police departments. If they pay attention to your report, if they ask these questions across the country, we'll be in a much better position to know what's to be done.[74]

[74] Maria Rasmussen, "Perceptions of Homeland Security Needs by Law Enforcement Executives in California," unpublished manuscript, CHDS, Monterey, June 05, 28.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS

I have divided my recommendations into two sections. The first describes four stages of growth for a sample Terrorism Working Group effort. These were developed with the assistance of Lt. John Sullivan of the Los Angeles County Sheriff's Department. The second describes the results of my participation in a Homeland Security Advisory Committee. My working group developed sample recommendations for fusion center implementation that are listed below.[75] Based upon the interviews conducted with the California Police Chiefs and Sheriffs, I have added their comments as appropriate.

Table 5. TEWG Growth Stages

Type 1	o Integrating concept (clarifying TEWG concept with Stakeholders o Monthly Meetings (for training and information sharing) o Committees/doctrine/IPO (Intelligence Preparation for Operation)
Type II	o Net Assessment for Special Events/specific threats o Workshops supplement monthly meetings (topics such as cyber-terrorism or suicide bombings)
Type III	o Full time staff o All-source Intel (open source, sensitive/classified/on-going investigations) o Multi-agency joint intel o Net Assessment Center
Type III (with Technology enabled)	o GIS, data-mining
Type IV	o Networked with other TEWs (node-to-node collaboration) o Distributed users/producers of intel

Effective intelligence/information fusion requires the following:

- The use of common terminology, and definitions by all stakeholders
- Up-to-date awareness and understanding of the global and domestic threat environment
- A clear understanding of the links between terrorism-related intelligence and Non-terrorism-related information (e.g., flight school training, drug trafficking) so as to identify those activities that are precursors or indicators of an emerging threat

[75] Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion," April, 2005.

- Clearly defined intelligence and information requirements with the Federal intelligence community that prioritize and guide planning, collection, analysis, dissemination, and reevaluation efforts
- Identifying critical information repositories2 and establishing the processes, protocols, procedures, and technical capabilities to extract information and/or intelligence from those repositories
- Reliance on existing information pathways and analytic processes as possible
- All-hazards and all-crimes approach to defining information collection, analysis, and dissemination
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process
- Understanding and elimination of impediments to information collection and sharing (i.e., it should be a priority for the Federal Government to provide State, local, and tribal entities unclassified terrorism-related information/intelligence so that it can be integrated into statewide and/or local fusion efforts)
- Capacity to convert information into operational intelligence
- Extensive and continuous interaction with the private sector and with the public at large
- Connectivity (technical and/or procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories at all levels of classification as necessary
- Extensive participation of subject-matter experts (SMEs) in the analytical process
- Capacity and commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties.

The fusion process is a key part of our nation's homeland security efforts. This process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. Simultaneously, it supports efforts to address immediate and/or emerging, threat-related circumstances and events. Although the collection, analysis, and dissemination of terrorism-related intelligence is not the sole

goal of the fusion process, one of the principal outcomes should be the identification of terrorism-related leads—that is, any nexus between crime-related and other information collected by State, local, tribal, and private entities and a terrorist organization and/or attack.

The fusion process does not replace or replicate mission-specific intelligence and information management processes and systems. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns and trends that may be indicative of an emerging threat condition. Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to State, tribal and local entities is that it will support ongoing efforts to address non-terrorism related issues by:

- Allowing State and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends;
- Supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities; and
- Improving the delivery of emergency and non-emergency services.

A. RECOMMENDED FUSION CENTER ATTRIBUTES

Fusion is a cyclical process that includes the following stages and activities. Flexibility is the key.

1. Management/Governance

- Define a management structure (e.g., who is in charge, what entity will manage and coordinate daily activities).
- Identify core (permanent) and ad hoc stakeholders.
- Design a governance structure advisory committee (multidisciplinary and multilevel of government).

- Define goals and objectives.
- Develop a process to define information and intelligence collection requirements.
- Develop the process and necessary memorandums of understanding to communicate requirements.

2. Planning and Requirements Development

- Conduct (and update frequently) a comprehensive and compatible risk assessment (threat, vulnerability, and consequence).
- Identify patterns and trends reflective of emerging threats.
- Define collection requirements based on results of risk assessments.
- Identify the circumstances or events (e.g., crime, public health) that represent indicators and/or precursors of threats.
- Identify the sources and/or repositories of data and information regarding indicators and precursors.
- Identify the existing capacity to collect key information from existing sources.
- Identify collection gaps and mitigate.
- Define public education, and other activities necessary to enhance situational awareness by the public.
- Develop training for front line law enforcement and other personnel so that they can better identify suspicious activities that may represent planning and/or operational activity by terrorist group.
- Ensure a mechanism exists to support reporting of collected information (e.g., 9-1-1, tip-line, Internet, connectivity to key information systems).
- Identify regulatory, statutory, privacy, and/or other issues that impede collection and sharing of information.
- Develop (in partnership with private-sector officials) detailed knowledge of vulnerabilities and consequence in the private sector to possible terrorist

attacks to assess the likelihood of attack, the likely methods of attack, the likely equipment and substances used to carry out such an attack, and identify planning activities.

3. Collection

- Communicate collection requirements to relevant State, tribal, local, and private sector entities.
- Implement situational awareness activities (e.g., training, public education).
- Mitigate impediments to collection.
- Compile classified and unclassified data, information and intelligence generated by people and organizations.
- Serve as the 24/7/365 initial point of contact for information provided by the U.S. Department of Homeland Security, Department of Defense, Department of Justice, Federal Bureau of Investigation, and other Federal entities (via telephone calls, Homeland Security Information Network/Joint Regional Information Exchange System, LEO, e-mail bulletins, VTC, fax) for the receipt of the following:
  - immediate threat-specific information (classified and unclassified)
  - Long-term threat information (classified and unclassified)
  - Tactics and methods used by terrorists (classified and unclassified)
  - Integrate with other reporting systems (e.g., 9-1-1, 3-1-1), and establish and maintain further, easy-to-use capability for the public reporting of suspicious activity in conjunction with the Joint Terrorism Task Force (e.g., internet, toll-free tip-line).
  - Establish a process to identify and track reports of suspicious circumstances (e.g., pre-operational surveillance, acquisition of items used in an attack).

4. Analysis

- Blend data, information, and intelligence received from multiple sources.
- Reconcile, de-conflict data, and validate as to credibility of data, information and intelligence received from collection sources.
- Evaluate and analyze data and information using SMEs.
- Identify and prioritize the risks faced by the jurisdiction (e.g., State, local).
- Produce value-added intelligence products that can support the development of performance-driven, risk-based prevention, response, and consequence management programs.
- Identify specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages.

5. Dissemination, Tasking, and Archiving

- Identify those entities and people (e.g., officials, executives) responsible for developing and implementing prevention, response, and consequence management (public and private) efforts.
- Provide relevant and actionable intelligence in a timely manner to those entities responsible for implementing prevention, response, and consequence management efforts (public and private sector).
- Archive all data, information, and intelligence to support future efforts.
- Support the development of performance-based prevention, response, and consequence management measures.
- Establish the capacity to track performance metrics associated with prevention, response, and consequence management efforts.
- Provide feedback to information collectors.

6. Reevaluation

- Track the achievement of prevention, response, and consequence management program performance metrics so as to evaluate impact on the risk environment.
- Update threat, vulnerability, and consequence assessments so as to update the risk environment.
- Assess effectiveness of national (i.e., Federal, State, tribal, and local) intelligence and information collection requirements process.

7. Modification of Requirements

- Modify collection requirements as necessary.
- Communicate modifications in a timely manner.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSIONS

Simply put…we have to connect the dots. On September 10, 2001, we knew the following information…

- Six Arab nationals were taking flying lessons
- None were doing well
- Two were disrupting the class
- Two said no need for take-off & landing training
- All wanted only Boeing aircraft training
- One was arrested in August 2001 by INS
- Three were stopped by CAPPS before boarding
- **and no system to connect the dots**

In December, 2003, the Markle Foundation issued their second report, "Creating a Trusted Network for Homeland Security."[76] Their words ring true, even today.

"Important information or analytical ability resides not just in the 15 intelligence components of the federal government and federal law enforcement and security agencies, but also…

- 17,784 state and local law enforcement agencies
- 30,020 fire departments
- 5,801 hospitals
- millions of first responders…on the frontlines of homeland security"[77]

I have skimmed the surface of available information regarding the intelligence/information sharing dilemma that we face today, not just in the law enforcement arena, but throughout the homeland security grid.

From JRIES/HSIN, to the RISS network, to the failed MATRIX project…there are database approaches that have worked to a degree and those that have failed miserably.

---

[76] Markle Foundation, "Creating a Trusted Network for Homeland Security," December 2003, http://www.markle.org/resources/reports_and_publications/national_security/index.php.

[77] Ibid.

It is very clear that taking a database approach and making it work is possible. The Los Angeles Terrorism Early Warning Group is taking steps toward accomplishing just that, a fusion process that works.

It still comes down to people however…people in leadership positions and people in black and white police cars. People at the local Health clinic and people in the Emergency room at the local hospital. The coordination and collaboration of the public and private sector entities discussed in this paper are what will make our country safer.

Interestingly, the responses of the California law enforcement leadership are most telling. The following is a compilation of the four groups, by department size:

- 77% stated that there was inadequate intelligence sharing between federal, state and local agencies
- 89% said that they had inadequate resources to accomplish that intelligence function
- 90% said that they lacked the proper training
- 67% were unaware of most federal databases
- 80% do not receive a daily intelligence briefing
- Yet, 78% said that they would somehow participate in a local "fusion" effort.

There is hope in those numbers. One Chief said it most eloquently, "Keep all the Suburbans and contamination gear, just give me a good intel analyst, someone who knows who to call and what to do with the info when they get it."

And what of the leadership role? Is transformational leadership the model that we must utilize to accomplish the law enforcement homeland security role in 2005. True leaders conquer the context, while managers surrender to it. What better analogy can we utilize to describe the state of homeland security and law enforcement today? The ability to adapt to unpredictable and chaotic change is the true mark of leadership in the law enforcement arena. As my survey indicates, the will is there, we just have to find the right way. There are many reasons to believe that transformational leadership just may be that way.

To some degree, the fusion process involves every level and sector (discipline) of government, the private-sector, and the public. The level of involvement from these

participants will vary based on specific circumstances. Some disciplines, such as law enforcement, represent a core component of the fusion process because of the relationship between crime and information sharing. In many cases, law enforcement authorities are best-suited to coordinate statewide and local fusion efforts. Minimally, the fusion process should be organized and coordinated on a regional level and each region should establish and maintain an analytic center to facilitate the process.

Each major urban area (as defined by the Urban Area Security Initiative [UASI] program) should establish a similar capacity ensuring it is interlinked with the fusion process established by the outlying regions. Other localities, tribal governments, and even private-sector entities should develop a process to interlink and participate in these regional (or UASI) fusion efforts. The public should be engaged through public education programs that describe what they should look for and what to do if they observe suspicious activities or circumstances.

Efforts should be organized and managed on a geographic basis and scalable so adjustments can be made based on changes in the operating and/or threat environment. While national standards and guidelines should guide the institutionalization of the process, the actual technological infrastructure and operational protocols used by individual jurisdictions should be based on the management structure, specific needs, and capabilities of each individual jurisdiction. One size does not fit all, but there are examples available that demonstrate successful approaches. We can no longer afford failure.

We invariably return to the essential question…How can we improve information and intelligence sharing at the local law enforcement level? While the word "improve" implies that there is an existing system or method, I am not sure that we are even able to make that statement in 2005. What I have suggested in this thesis are possibilities. There is, perhaps, a way to accomplish the necessary and vital process for the real-time and consistent information flow between federal, state and local entities.

While the lack of information and intelligence sharing has been excruciatingly dissected since September 11, 2001, we have made halting steps toward a functional system. I began my discussion with three options. While the Super-Agency approach has worked in other countries and had been intricately studied in this one, I believe the

end result may be a refinement of the FBI domestic intelligence function, rather than the creation of an American version of MI-5. The role of law enforcement in foreign policy cannot be understated and except for the enormous reach of the New York City Police Department, no municipal law enforcement agency has the resources to play but a supporting role.

The Legal Reform approach offers programmatic rather than structural changes. The Patriot Act I and II, with the accompanying civil liberties controversy, provided numerous tools for accomplishing the homeland security mission, but as stated by Deputy Commissioner Cohen, "The Patriot Act helps the FBI do its job. And that is good for us. I'm too busy to see if the FBI abuses its power."[78] The point being that the legal reforms that I discussed previously deal mainly with the federal approach rather than a direct effect on state or local agencies.

The Database approach holds the key, since it can be adaptable nationwide. Within the Department of Homeland Security, sharing information so that different federal, state and local agencies all have access to the same data, when appropriate, is not just a good idea – it is the law. More precisely, it is the basis for a series of presidential directives and part of the overall strategy at DHS.

"It has been the highest priority, or among the highest priorities, since the formation of the Department."[79]

According to Holcomb, there has been enormous technical progress and some significant success in DHS information sharing. An example is the sharing of terrorist watch lists. Partnering between federal departments has led to a unified screening database, creating a definitive source within DHS that is readily available to those that need it. Holcomb also believes that advances in hardware and software have removed many of the technological barriers to information sharing.[80]

On the flip side, retired Lieutenant John Aerts of the Los Angeles County Sheriff's Department, offers a slightly different view. Aerts was involved with the Department of Justice task force on the global Justice XML data model standard

[78] David Cohen (Deputy Commissioner, NYPD), CNN Interview April 2005.

[79] Lee Holcomb (Chief Technology Officer, Department of Homeland Security), Interview with author, May 2005.

[80] Ibid.

(GJXDM). "There is no technology issue. Using the global justice model and the tool sets for sharing data and analyzing data, any of this can be accomplished anywhere. The issue always comes down to politics and turf." [81]

These contrasting views provide a perfect summary of the state of information sharing today. We may have the technical ability to share vast amounts of information today, but we do not yet have the political or jurisdictional means to get it done.

What we do have are existing networks, each well-known in narcotics enforcement circles, that may provide the framework for advancement. RISSnet, RISS ATIX, JRIES/HSIN all have enormous potential and existing frameworks. As is often the case in law enforcement, however, the overall knowledge of these systems is lacking (as evidenced by the Chiefs and Sheriffs responses to the questions regarding existing databases) and the political will is not yet there.

Where there is political will and leadership, there exists a model framework that has promise. The Los Angeles TEW model provides one example that holds promise for success. While the metrics that measures that success are still nebulous (the measurement of prevention efforts will always be difficult), the transformational leadership and teamwork demonstrated by the LA TEW can be emulated using similar models.

Thus, the more generic outline of fusion center attributes and stages that can serve as a guide for any information sharing effort, whether it be large or small, urban or rural.

If we can overcome the problems of funding, politics, jurisdictions and technology and have universal data analysis, relevant information sharing and effective transformational leadership, we will have taken a major step toward the ultimate goal – a functional homeland security system.

[81] John Aerts (retired Lieutenant, Los Angeles County Sheriff Department), Police Magazine, April 2005.

THIS PAGE LEFT INTENTIONALLY BLANK

APPENDIX

VENTURA POLICE DEPARTMENT
Training Bulletin 05-11

California State Warning System – Terrorism Information

As the result of a Presidential Directive to improve communication between Local and Federal law enforcement, the Federal Bureau of Investigation, the California State Office of Homeland Security, and the California Highway Patrol have created a program to provide local law enforcement officers direct and timely access to FBI and other Federal databases that relate to terrorism. This service can be accessed through the **California State Warning Center** and will be available 24 hours a day, 7 days a week.

Local law enforcement officers in the field will receive real time information relative to potential terrorism related subjects and any other information that could be beneficial to an ongoing investigation. The program is designed to assist local law enforcement officers who are making traffic stops or conducting investigations of suspicious addresses or subjects. The program is designed to identify whether the individual(s) or circumstances may be related to terrorist activities.

Local law enforcement dispatch centers call the center, provide the data, and should receive information on what action the officer in the field should take. This could vary from taking no action, completing an FI and release, or detaining the individual for an FBI agent to interview the subject. The return should be within 20 minutes depending on the nature of the information.

Procedure for accessing this information:

- Telephone the California State Warning Center:
- The requestor must provide verification of law enforcement status, their Originating Agency Identifier (the Ventura Police ORI is CA0XXXXX), and an agency call back number.
- Depending on the circumstances, the request will be classified as requiring either an immediate or routine response from the FBI Counter Terrorism Watch.
- The Counter Terrorism Watch will query various Federal databases and the CATIC databases in an effort to determine if the subject, phone number, or address is of interest.
- The Counter Terrorism Watch will provide guidance as to what course of action is to be taken as it relates to the queried subject. The return call should occur in approximately 20 minutes.

Additionally, all developed information will be forwarded to the local FBI Joint Terrorism Task Force for further action regardless of the initial directives provided to the officers in the field at the time.

Ventura Police Officers who access and utilize this will complete the VPD Narcotic/Terrorist Intelligence form and forward it to Training Unit sergeant.

LIST OF REFERENCES

Al-Qaeda Training Manual. (http://www.usdoj.gov/ag/trainingmanual.htm), last accessed March 22, 2005.

Barry, Dan. "The Giuliani Years: The Overview – A Man Who Becomes More Than Mayor." *New York Times*, December 31, 2001.

Bass, Bernard M. "Does the Transactional -- Transformational Leadership Paradigm Transcend Organizational and National Boundaries?" *American Psychologist* 52, no. 2 (1997).

_____. *Transformational Leadership.* New York: Lawrence Erlbaum and Associates, 1997.

Bellavita, Christopher. NS 3180 Lecture, Naval Postgraduate School, Monterey, CA. April, 2004.

_____. "The Public Administrator As Hero." *Administration and Society.* Vol. 23, No.2 (August 1991).

Bennis, Warren and Nanus, Bert. *Leaders: Strategies for Taking Charge.* New York: Harper and Row, 1985.

Bennis, Warren. *Managing the Dream: Reflection on Leadership and Change.* Cambridge, MA: Perseus Publishing, 2000.

_____. *On Becoming a Leader.* Reading, MA: Perseus Publishing, 1994.

Bergstein, Brian. "Database Firm Tagged 120,000 Terrorism 'Suspects' for Feds." *Biloxi, MS Sun-Herald*, May 20, 2004.

Bodrero, Douglas. "Law Enforcement's New Challenge to Investigate, Interdict, and Prevent Terrorism." *The Police Chief* (February 2002).

Brannan, David W. *Beyond International Terrorism: Thinking About the 'Domestic' vs. 'International' Divide.* Oklahoma City: MIPT, 2003.

Burns, James McGregor. *Leadership.* New York: Harper and Row, 1978.

Calvin, James R. "Leadership Networking and Active Transitions in the Workplace: Freedoms, Energy and Transformative Relationships." *SAM Advanced Management Journal* 68, No. 4 (2003).

Church Committee Final Report. "Intelligence Activities and the Rights of Americans." April 23, 1976. http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportfindings.htm.

Gardner, Howard and Laskin, Emma. *Leading Minds – An Anatomy of Leadership.* New York: Basic Books, 1996.

Gill, Roger, Levine, Niall and Pitt, Douglas. "Leadership and Organizations for the New Millennium." *Journal of Leadership Studies* 5, No. 4 (1998).

Gilmore Commission Report. "The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction" (Fifth Annual Report, RAND Corporation, December 15, 2003), http://www.rand.org/nsrd/terrpanel/. Last accessed March 9, 2005.

Hargrove, Robert. *E-Leader: Reinventing Leadership in a connected Economy.* Cambridge, MA: Perseus Publishing, 2001.

Hoffman, Bruce. *Combating Terrorism: In Search of a National Strategy.* Testimony before the House Committee on Government Reform, March 2001.

Hollander, Edwin. *The Balance of Leadership and Followership (*Academy of Leadership Press, 1997). http://www.academy.umd.edu/publications/klspdocs/follower_intro.htm, last accessed March 23, 2005

Homeland Security Advisory Council. "Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion." April 2005.

Howitt, Arnold M. and Pangi, Robyn L. Editors. *Countering Terrorism: Dimensions of Preparedness.* Cambridge, MA: Belfer Center for International Affairs, John F. Kennedy School of Government, Harvard University, 2003.

Hunt, James G. *Leadership: A New Synthesis.* Newbury Park, CA: Sage Publications, 1996.

International Association of Chiefs of Police. *Criminal Intelligence Sharing Report.* August 2002.

Lynch, Michael. "Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State, Local Governments." Senate Intelligence Committee Hearing Statement, March 23, 2005.

Markle Foundation. "*Creating a Trusted Network for Homeland Security."* December 2003. http://www.markle.org/resources/reports_and_publications/national_security/index, last accessed July 23, 2005.

National Narcotic Officers' Association Coalition. "Regional Information Sharing Program." *NNOAC Insight, April 2005.*

National Strategy for Homeland Security. Washington, D.C.: Office of Homeland Security, July 2002.

O'Harrow, Robert Jr. "Anti-Terror Database Got Show at White House," *Washington Post,* May 21, 2004.

Pelfrey, William. Unpublished Paper. 2004.

Pentagon Papers. *New York Times*, 1971, http://www.infoplease.com/ce6/history/A0838198.html.

Rasmussen, Maria. "Perceptions of Homeland Security Needs by Law Enforcement Executives in California." Unpublished manuscript, CHDS, Monterey, June 05.

Robinson, Brian. "DHS Unfolds Safety Net." *Federal Computer Week,* June 21, 2004.

Rood, Justin. "Pentagon Has Access to Local Police Intelligence Through Office in Homeland Security Department." *CQ Homeland Security,* July 6, 2004.

Sarkar, Dibya. "HSIN Starts Five Months Early," *Federal Computer Week,* July 8, 2004.

Sashkin, Marshall. *The Visionary Leader.* Bristol, Connecticut: New World Press, 1998.

Schwartz, John. "Privacy Fears Erode Support for a Network to Fight Crime," *New York Times,* March 15, 2004.

Sullivan, John. Los Angeles County Sheriff's Department, Naval Postgraduate School Presentation, January 2005.

Torr, James D. (ed.) *Homeland Security: At Issue Opposing Viewpoints Series*. New York: Thompson Gale, 2004.

Ulrich, Andreas. "Radical Islam's Rising War on Europe." *Der Speigel* (July 12, 2005), http://www.salon.com/news/feature/2005/07/12/terrorism_eu/print.html, accessed July 12, 2005.

U.S. Department of Homeland Security. "Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities," Press Release, Feb. 24, 2004.

U.S. Department of Justice, Bureau of Justice Assistance. "The RISS Program: 2002 Membership and Service Activity." CFR Part 23. Washington D.C., June 2003.

U.S. Department of Justice, Bureau of Justice Assistance. "Regional Information Sharing Program." *Bureau of Justice Assistance Program Brief.* Washington, April 2002.

U.S. Department of Justice, Bureau of Justice Assistance. "The RISS Program: 2002 Membership and Service Activity." Washington, June 2003.

U.S. Department of Justice, Office of Justice Programs. *The National Criminal Intelligence Sharing Plan.* Washington, October 2003.

Ventura County Terrorism Response Plan. November 2001.

Welsh, William. "Feds Offer to Mend Matrix," *Washington Technology,* May 24, 2004.

White, Jonathan. *Defending the Homeland*. Belmont, CA: Wadsworth, 2004.

THIS PAGE LEFT INTENTIONALLY BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California